bag to the database **26**. The database **26** then associates the GUID (global universal identifier) and the rentalid of the updated rental bag in its database, thereby rendering that content item playable upon that device **18**. The database **26** then sends the updated rental bag to the client device **18**.

[0027] Provided in one embodiment is a security check procedure to attempt to defeat hackers, who try to use the system in unauthorized fashion, such as tampering with the content. This procedure is invoked for both check in and check out and does require initially detection by the system of tampering; this detection is part of the DRM process.

[0028] For check in, when the client first accesses the rental database, an element ("flag" in software terminology) is provided in the DRM data indicating the possible detected tampering. The content database then sends the rental bag to the DRM server with this indication. The DRM server then determines if there has been in fact tampering, and if so sends an indication (another flag) back to the content database. The content database maintains a flag counter for this type of flag for each item, and increments the counter upon receipt of each such flag. If the counter value exceeds a predetermined threshold, then that rentalid is excluded so that content item for that device is rendered unplayable. A warning or notice may be provided to the user at this point.

[0029] A similar security process is provided for the check out procedure. The check out here is modified so that when the content database checks whether the rental bag is eligible for check out, if it determines that the content item is already checked out to that GUID, then the transaction is excluded. Further, if the flag counter value for the rental is greater than the threshold, the transaction is excluded as above. If the value of the flag counter is below the threshold, the content is allowed to be played but the counter value is incremented. Again, a warning or notice may be provided to the user.

[0030] In accordance with another aspect, two embodiments are provided for respectively higher/lower levels of security. In the lower security embodiment, when the user elects to play the rented content, the relevant key bag for the entire rented item is downloaded to his client device and stored there. He can then play the content, even if thereinafter his client device is no longer in communication with the iTunes Store (e.g., the client device is no longer connected to the Internet). In the higher security embodiment, the keys are downloaded only as needed for each portion of the rented item, so the client device must remain in communication with the iTunes Store.

[0031] This disclosure is illustrative but not limiting. Further modifications will be apparent to those skilled in the art in light of this disclosure and are intended to fall within the scope of the appended claims.

1-16. (canceled)

17. A method comprising:

transmitting a request for content to a server;

receiving at least a portion of the content from the server in an encrypted form;

receiving a rental key from the server, the rental key being valid for a first period of time during which play back of the content can be initiated;

upon transmitting, to the server, a request to initiate play back of the content within the first period of time, receiving, from the server, a decryption key that enables play back of the content over a second period of time; and

receiving, based at least in part on the first period of time associated with the rental key and the second period of time associated with the decryption key, at least another portion of the content in encrypted form during the second period of time.

18. The method of claim **17**, further comprising:

decrypting the at least the portion of the content using the decryption key; and

presenting, the decrypted at least the portion of the content.

19. The method of claim **17**, wherein the first period of time is thirty days and the second period of time is twenty-four hours.

20. The method of claim **17**, wherein the decryption key is transmitted in a key bag data structure.

21. The method of claim **20**, wherein the key bag data structure stores a plurality of decryption keys for decrypting a plurality of portions of the content in the encrypted form.

22. The method of claim **17**, wherein the decryption key is not received when the request to initiate play back of the content is transmitted after the first period of time has expired.

23. The method of claim **17**, further comprising:

receiving a security policy along with the decryption key, wherein the security policy specifies at least one of: a maximum number of times the decryption key may be used to decrypt the at least the portion of the content over the second period of time, or a maximum number of client devices on which the decryption key may be used to decrypt the at least the portion of the content.

24. The method of claim **17**, wherein the content comprises video content.

25. The method of claim **17**, wherein the second period of time is different than the first period of time.

26. The method of claim **17**, wherein, during the second period of time, the decryption key enables play back of the content without communication with the server.

27. The method of claim **17**, wherein, during the second period of time, the decryption key enables play back of the content only when in communication with the server while play back occurs.

28. The method of claim **17**, wherein receiving the at least the other portion of the content comprises receiving a content stream that includes the at least the other portion of the content.

29. A non-transitory machine-readable medium comprising code that, when executed by one or more processors, causes the one or more processors to perform operations, the code comprising:

code to transmit a request associated with accessing content to a server;

code to receive, from the server in response to the request, a rental key that is valid for a first period of time during which play back of the content can be initiated;

code to, upon transmitting, to the server, a request to initiate play back of the content within the first period of time, receive, from the server, a decryption key that enables play back of the content over a second period of time; and